P R O M E M O R I A

Datum 2021-03-04 FI Dnr 20-3685
Författare Finansinspektionen

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Cyberhot och finansiell stabilitet – FI:s roll och uppgifter

Innehåll

Sammanfattning

På senare tid har ett flertal olika lagförslag och andra initiativ presenterats i syfte att stärka den finansiella sektorns motståndskraft mot cyberattacker. Mot den bakgrunden har Finansinspektionen (FI) tagit fram denna promemoria som beskriver vilken roll FI har när det gäller att bidra till en hög cybersäkerhet samt hur arbetet för att motverka cyberhot mot den svenska finansiella sektorn ser ut.

De senaste decenniernas digitala utveckling innebär stora möjligheter, men ställer samtidigt krav på att hantera de risker som utvecklingen för med sig. Riskerna förstärks dessutom av en delvis försämrad säkerhetspolitisk situation. FI kan konstatera att cyberhot är en uppenbar risk som varje finansiellt företag i sitt eget intresse måste hantera. Vi ser också att det finns risker för negativa externa effekter, det vill säga att varje enskilt företag inte har incitament att fullt ut ta hänsyn till hur en cyberattack mot det enskilda företaget kan påverka samhällsekonomin. Därmed finns samma grundläggande motiv för FI att agera på detta område som när det gäller risken för en traditionell finanskris.

Eftersom den finansiella sektorn i väldigt hög grad är digitaliserad har cybersäkerhet blivit en viktig fråga för de finansiella företagen på senare tid. Givet den finansiella sektorns centrala roll i samhället är cybersäkerhet i finanssektorn en angelägenhet för hela samhället. Det faktum att de finansiella företagen och marknaderna är nära sammanlänkade med varandra, och att eventuella problem därför snabbt kan sprida sig, gör att behovet av samverkan här är än större. Mot denna bakgrund finns det skäl att utveckla myndigheternas samverkan mot cyberrisker i den finansiella sektorn.

FI har redan i dag, med den nuvarande lagstiftningen, flera olika verktyg för att hantera cyberrisker i de företag som är under vår tillsyn. Dessa befogenheter varierar dock mellan finansmarknadens olika sektorer. Under andra halvåret 2020 föreslogs nya regler inom EU som kommer att påverka tillsynen av de finansiella företagens cyberrisker. Dessutom pågår en återuppbyggnad av det svenska totalförsvaret. Detta ställer krav på myndigheter, däribland FI, att vidta åtgärder för att öka motståndskraften mot cyberrisker.

1. Hur ser cyberhoten ut?

Komplext och mångfacetterat
Problem relaterade till cyber- och it-risker är av skiftande karaktär och kan klassificeras på olika sätt. Ett sätt är att dela upp problematiken i två huvudformer, dels rena tekniska problem och handhavandeproblem, dels cyberattacker, det vill säga medvetet skapade störningar för att komma över pengar eller information, manipulera uppgifter eller för att sabotera verksamheten i enskilda företag eller i ekonomin i stort. Detta betecknas ofta som icke-antagonistiska respektive antagonistiska störningar. Exempelvis kan antagonistiska attacker utföras av en statlig aktör för att skada ett annat land. Bägge varianterna kan i sin tur ta sig många former och kan drabba i princip alla verksamheter och samhällsfunktioner.[1]

Det finns en allmän uppfattning om att betydelsen av bägge typerna av risker har ökat och fortsätter att öka.[2] Detta trots en växande medvetenhet och en snabb utveckling av riskhantering samt av säkerhetstekniker och säkerhetsrutiner. Sårbarheten till följd av oavsiktliga störningar ökar främst som en reflex av att beroendet av it och av digitala nätverk ökar snabbt inom samhällets alla områden – inte minst på det finansiella området. Betydelsen av antagonistiska störningar växer av delvis samma skäl. Men att de antagonistiska störningarna blir allt viktigare beror också på att angreppen blir mer och mer sofistikerade och att vinsterna eller påverkan av en attack kan vara stora samtidigt som riskerna för förövarna ofta bedöms vara måttliga.

Slutligen finns goda skäl att anta att denna typ av risk är, och alltmer blir, ett problem inte enbart för de enskilda finansföretagen, utan för den finansiella sektorn som helhet. FI behöver utveckla ett systemövergripande synsätt och arbete, utöver den mer företagsspecifika tillsyn som vi - i växande grad – har utövat sedan länge. Finansiell reglering och tillsyn kan bidra till att minska sårbarheten för cyberrisker på ett viktigt område, men det förutsätter ett brett samarbete med olika aktörer, såväl privata som offentliga.

Cyberattacker i fokus
Det finns flera likheter när det gäller effekterna av oavsiktliga respektive avsiktligt skapade it- och cyberproblem. Ett datasystem eller nätverk som havererar på grund av felhantering eller tekniska problem får i varje fall i teknisk mening samma effekt som om samma haveri initieras av någon illasinnad. Dessutom är en god nivå på den rent operativa säkerheten ett sätt att bygga motståndskraft och robusthet även mot attacker. Till detta kan läggas att oavsiktliga, mer vardagliga störningar i kvantitativ mening kan ses som ett

[1] Financial Stability Board (FSB) har i sitt Cyber Lexicon från 2018 definierat ett flertal olika termer när det gäller cybersäkerhet inom den finansiella sektorn.
[2] Se exempelvis https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/ (läst 2021-01-27) eller Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM(2020) 823 final. s. 1

större problem, eftersom det är något som händer överallt och på daglig basis, medan i varje fall mer omfattande attacker fortfarande är ovanliga.

Det som motiverar att attacker ändå förtjänar ett särskilt fokus och kräver en i viss mån separat hantering, är att de adderar ytterligare en riskdimension utöver de traditionella operativa riskerna. Detta tillför ytterligare en nivå av komplexitet – analytiskt, juridiskt, tekniskt och organisatoriskt. I nuläget bedöms sannolikheten vara större för att en incident med bredare, mer samhällspåverkande och systemhotande konsekvenser, till exempel ett haveri i betalningssystem, skulle uppstå till följd av en teknisk incident än av en attack utförd av främmande makt, en terrorgrupp eller kriminell organisation.

Skadorna av en antagonistisk attack kan dock väntas bli större. En viktig orsak till detta är att en aktör som utför en attack har en medveten ambition att åstadkomma så svåra och omfattande skador som möjligt, medan aktörerna på marknaden har starka incitament i motsatt riktning, det vill säga att både minska risken för problem och att hantera dem så effektivt som möjligt om de ändå uppstår. Dessutom kan en antagonistisk attack få större psykologiska och politiska konsekvenserna, och därmed påverka förtroendet mer. Mot den bakgrunden är det rimligt att i detta sammanhang lägga fokus på de risker som är förknippade med avsiktliga störningar av de digitala funktioner som är kritiska för den finansiella sektorn. Det är de antagonistiska störningarna, det vill säga cyberattacker, som är fokus för denna strategi.

Det har inträffat ett betydande antal kända cyberattacker mot finansiella företag och marknader av mer eller mindre allvarligt slag – och med stor säkerhet också ett antal okända sådana. Ingen av dessa incidenter, eller kombination av incidenter, har fått systemhotande konsekvenser. Det är dock ingen garanti för att något sådant inte kommer att kunna hända i framtiden.[3]

Några typer av incidenter och attacker som skulle kunna inträffa är bland andra följande:

- Attack för att undergräva förtroendet i och för finansmarknaden genom att exempelvis skapa falska nyheter, ryktesspridning och desinformation i sociala medier, falska mejl från banker eller myndigheter eller genom attacker på nyhetersbyråer som Reuters och Bloomberg och andra leverantörer av kritiska data relaterade till finansiella tjänster.
- Attacker för att manipulera, förstöra eller offentliggöra data, exempelvis personuppgifter.
- Attack mot uttagsautomater, nationella leverantörer av identifieringstjänster (till exempel Bank-id) eller betalningstjänster (till exempel Swish).

[3] I Europeiska kommissionens cybersäkerhetsstrategi från 2020 anges finanssektorn som en av de mest utsatta sektorerna när det gäller cyberattacker (Se Gemensamt meddelande till Europaparlamentet och Rådet, EU:s strategi för cybersäkerhet för ett digitalt decennium, JOIN(2020) 18 final, s. 3).

- Attack mot eller genom det globala meddelandesystemet för betalningar (Swift).

Vissa typer av incidenter och attacker kan påverka den finansiella sektorn även om de inte är direkt riktade mot den. Som exempel kan följande nämnas:

- Attack mot kritiska tekniska komponenter (till exempel operativsystem, applikationer och kommunikationsprotokoll för internet samt lagringstjänster) som används av de flesta finansiella institut och dess tjänsteleverantörer.
- Attack mot tredjepartsleverantörer som levererar kritiska finansiella tjänster, till exempel molntjänster, till flera systemviktiga aktörer på den finansiella marknaden, som leder till att tjänsterna blir otillgängliga under en längre period. Detta kan också ta formen av uppköp och övertagande av viktiga tredjepartsleverantörer.
- Attack som slår ut annan kritisk nationell infrastruktur som till exempel energi och telekommunikation, vilket leder till att de finansiella tjänsterna blir otillgängliga under en längre period.

Hur skiljer sig cyberrisker från andra stabilitetsrisker?
Riskerna för finanssektorns del är mångfacetterade och svåra att överblicka, bedöma och hantera med traditionella verktyg. Exempelvis skulle en cyberincident kunna uppstå på sekunden utan någon förvarning och drabba större delen av finanssektorn samtidigt. Då blir det svårt eller omöjligt att applicera traditionella verktyg i tid och begränsa spridningen, vilket oftast är möjligt vid finansiella kriser i de former som de har uppträtt hittills. Vidare hör det till bilden att cyberattacker, liksom icke-antagonistiska operativa risker, bara innebär nackdelar, till skillnad från traditionella finansiella risker som kreditrisker och marknadsrisker.

En annan aspekt är att kunskaperna är mycket ofullständiga, kanske i synnerhet när det gäller interaktionen mellan olika företag och olika delar av det finansiella systemet när en störning inträffar. Vidare är tillgång och jämförbarhet när det gäller relevanta data begränsad. Det beror bland annat på att det – återigen till skillnad från traditionella finansiella risker – varken finns något utvecklat teoretiskt ramverk, tydliga och etablerade definitioner eller någon längre historia att bygga på. Dessutom har, som nämnts, ingen stor systemkritisk störning inträffat än så länge, så även den erfarenheten saknas. Detta innebär bland annat att möjligheterna till statistiskt baserad analys – normalt en central del i finansiella riskbedömningar – blir begränsade.

Men det finns fler speciella drag i riskbilden. Utan något försök till inbördes betydelseordning kan man peka på dessa:

- Störningar kan pågå, spridas och interagera även utan mänskliga ingrepp, och utan hinder av geografiska och institutionella gränser.
- Det är ofta svårt att klarlägga när, var, hur och varför en störning har uppkommit och hur den spridits.

- Det är svårt att identifiera och bedöma effekter och kostnader, i synnerhet de som är mer indirekta och långsiktiga. Därmed är det också svårt att prissätta riskerna.[4]
- Effekterna av många var för sig mindre störningar eller angrepp, som kanske inte får några drastiska konsekvenser för var och en av de enskilda aktörerna, kan sammantagna skapa stora förtroende- och funktionsskador för marknaden som helhet.
- Det finns kontraproduktiva incitament – företag är ofta av konkurrensskäl ovilliga att informera om problem de drabbats av.

Finansiella marknader och företag är finansiellt nära sammanlänkade, till exempel i form av transaktionshantering, ömsesidiga krediter, beroende av samma marknader och infrastrukturer.[5] Därtill har de enskilda aktörerna vare sig tillräcklig överblick eller tillräckliga incitament för att ta höjd för de risker som uppstår genom interaktionen mellan olika delar och aktörer i systemet. Därför blir en aktörs problem lätt allas problem. Cyberhot förstärker dessa sammanlänkningsrisker på flera sätt. Den kanske viktigaste faktorn är att de finansiella tjänsterna i sin helhet är beroende av tekniska system som är globalt sammankopplade med hög komplexitet och låg transparens, och till stora delar exponerade mot internet. Tekniska lösningar, programvaror etc. är också i hög grad gemensamma.

Tekniken gör således ett redan tidigare starkt sammanlänkat system ännu mer sammanlänkat, samtidigt som de otillräckliga incitamenten för en riskhantering på systemnivå kvarstår. Det blir även allt tydligare att de finansiella företagen också utsätts för risker länkade framför allt till kritiska underleverantörer, men också till kunder, samhällelig infrastruktur och egna anställda. Man kan alltså konstatera att riskerna i viktiga delar befinner sig utanför det enskilda företagets egen kontroll.[6] Sammanlänkningsdimensionen, i synnerhet i kombination med risken för uppsåtliga angrepp, är alltså en grundläggande systemmässig sårbarhet när det gäller cyberrisker. Cyberriskerna kan också sammanfalla, förstärkas och samspela med andra, mer traditionella typer av risker och sårbarheter.

[4] Internationella valutafonden (IMF) menar i en studie att 90 procent av kostnaderna är indirekta, dock utan att närmare definiera dessa eller hur de har beräknats.
[5] Sammanlänkningen skapar i sig externaliteter. Svag riskhantering i ett företag påverkar även andra företag negativt. Omvänt skapar en god riskhantering positiva externaliteter som gynnar andra företag, som därmed kan sägas åka snålskjuts på andra företags riskhantering vilket i värsta fall minskar deras incitament att göra något själva
[6] Oliver Wyman, Combatting the Cyber Threat in Sweden – An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector, s. 4–5.

2. Cyberrisker, finansiell stabilitet och FI:s roll

FI har sedan länge – med tiden i ökande grad – arbetat med cyberrisker inom ramen för den löpande tillsynen av de finansiella företagen. Frågan diskuteras också regelbundet i det Finansiella stabilitetsrådet, där vi deltar med andra stabilitetsvårdande myndigheter.[7] Men i takt med att den här typen av risker hamnar mer och mer i fokus i kraft av deras växande betydelse för all slags finansiell verksamhet, finns anledning att också fundera över och diskutera hur en strategi för FI:s roll och uppgifter på detta område bör se ut.

I detta kapitel diskuteras FI:s roll när det gäller att hantera finansiella företags cyberrisker samt kopplingen mellan denna risk och finansiell stabilitet. I kapitlet diskuteras även vilka verktyg som behövs för att kunna hantera cyberrisker inom den finansiella sektorn, samt i vilken mån FI eller andra aktörer förfogar över dessa verktyg i dagsläget.

Risker på olika nivåer

Den finansiella marknaden och de företag som verkar där arbetar och fungerar i de flesta avseenden som andra företag i näringslivet. Men den finansiella sektorn och den finansiella verksamheten har vissa speciella egenskaper, som innebär olika slag av så kallade marknadsmisslyckanden, det vill säga risker som de enskilda företagen inte fullt ut har incitament och möjlighet att överblicka och hantera, och som kan leda till att skyddsnivåerna blir för låga ur ett samhällsekonomiskt perspektiv.

I värsta fall kan det leda till att centrala funktioner i det finansiella systemet slås ut, något som brukar kallas systemrisk. Detta inträffar om och när den operativa eller finansiella motståndskraften i företagen eller på marknaderna inte räcker för att absorbera en chock och rimligt snabbt återhämta sig ifrån den. Då kan den spridas vidare på ett mer eller mindre okontrollerat sätt, vilket i slutänden drabbar produktionen och sysselsättningen i hela ekonomin. De risker för allvarliga marknadsmisslyckanden som finns på finansmarknaden är det huvudsakliga skälet till att marknaden regleras och är föremål för statlig tillsyn på ett sätt som har få, om ens några, motsvarigheter i andra branscher.

Är cyberrisker en systemrisk?

Cyberrisker är uppenbart en risk som finansiella företag i sitt eget intresse måste ta höjd för och hantera. Nästa fråga är då om riskerna är av en karaktär att de kan hota systemets funktionsförmåga och stabilitet, eller om de ”bara” är ett problem för de enskilda företagen. Att det, som framgått, finns faktorer i detta som ett enskilt företag inte kan eller har incitament att hantera indikerar att företagsövergripande risker finns, men det innebär inte med självklarhet att dessa risker är så stora att de kan klassas som systemrisker och kräva någon form av särskild reglering. Frågan lär inte kunna få ett helt entydigt svar så länge som det saknas historisk evidens i form av en faktisk systemhotande

[7] Förutom FI ingår Riksbanken, Riksgälden och Regeringskansliet (Finansdepartementet) i det Finansiella stabilitetsrådet. Mer om rådet och dess arbete finns i kapitel 3 nedan.

attack. Samtidigt kan här, som antytts, även mer begränsade störningar, och bristande kapacitet att hantera sådana, skada systemets funktionsförmåga. Det kan innebära stora samhällsekonomiska kostnader utan att det för den skull leder till en akut systemkollaps. Även icke-systemstabilitetshotande negativa externaliteter kan alltså leda till betydande samhällsekonomiska skadeverkningar.

Utifrån olika studier som gjorts, kan det konstateras att det ännu inte finns någon enhetlig syn på hur länkarna till de finansiella systemstabilitetsriskerna ser ut, och om de i så fall är direkta eller enbart indirekta. Exempelvis hävdas i en studie från Bank of England att det framstår som osannolikt att enskilda attacker från privata aktörer ska kunna skapa systemkriser. Enligt studien kan bara statliga aktörer ha den kapaciteten och de anses inte vara fokuserade på att störa finansiella system i första hand.[8]Andra har gjort annorlunda och mer pessimistiska bedömningar.[9] Även när det gäller statliga aktörers intresse för att attackera den finansiella sektorn finns det bedömare som menar att finanssektorn kan vara ett viktigt mål.[10]

Det kan självklart diskuteras om en cyberattack direkt kan slå ut ett finansiellt system, eller om problem av den karaktären leder över i och transformeras till exempelvis kredit- eller likviditetsrisker, som i sin tur skapar systemrisk. I mer praktisk mening kan man hävda att detta är av sekundärt intresse; det är viktigt nog om, och på vilket sätt, en störning av den karaktären i varje fall kan fungera som en utlösande faktor.

Andra aspekter som är viktiga att beakta i sammanhanget är exempelvis

- vilka typer av funktioner och vilka typer av företag som är mest känsliga för cyberrisker
- vilken roll och betydelse dessa funktioner och företag har i ett systemperspektiv
- hur transmissionsmekanismerna till andra företag och sektorer ser ut.

Här är kunskapsläget i dag ganska bristfälligt, men några indikationer på vilka delsektorer som kan antas vara mer riskutsatta och som kan bli särskilt problematiska i ett systemperspektiv framgår av nedanstående sammanställning.

---

[8] Bank of England, Could a cyber attack cause systemic impact in the financial sector?, Quarterly Bulletin 2018, Q4.

[9] Se exempelvis danska Finanstilsynet som bedömt att hotet från cyberrisk är mycket hög (Strategi *for den finansielle saktors cyber- og informationssikkerhed 2019-2021*). Finanstilsynet (2019). IMF hävdar att "… cyber risk is a significant threat to global financial stability". (*"Cyber Risk, Market Failures and Financial Stability"* IMF 2017).

[10] "The US Intelligence Community estimates that there are now more than thirty countries with "military-grade destructive attack capability".9 Moreover, it concluded that the financial sector would be a prime target in the case that nations openly engage in cyber-warfare. By attacking the financial system, destruction and disruption of vital functions could be achieved, potentially resulting in widespread panic." Se Oliver Wyman, Combatting the Cyber Threat in Sweden - An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector, s. 6.

Typ av företag	Betydelse för finansiell stabilitet	Lockande för uppsåtliga aktörer	Kommentar
Större banker	Hög	Hög	• Banker utgör ofta en lockande startpunkt för uppsåtliga aktörer. • En attack kan få stor påverkan på den finansiella stabiliteten på grund av koncentrationen till ett fatal systemviktiga aktörer.
Betaltjänst-leverantörer	Hög	Hög	• På grund av direkt påverkan på konsumenter och hyfsat hög koncentrationsgrad, kan ett angrepp på betalningsleverantörer leda till att förtroendet för det finansiella systemet skadas. • Eftersom kontantbetalningar i Sverige gradvis fasas ut kan ett angrepp på betalningsleverantörer få en stor påverkan på grund av bristen på utbytbarhet.
Finansiell infrastruktur (börser, centrala motparter, transaktionsregister, clearingorganisationer)	Hög	Medium till Hög	• Företag inom den finansiella infrastrukturen utför ofta kritiska tjänster för vilka det finns ett fatal eller inga substitut. Ett angrepp mot dessa företag kan därför få stor påverkan på den finansiella stabiliteten.
Tredjeparts-leverantörer	Hög	Medium till Hög	• Ett angrepp på tredjepartsleverantörer kan innebära långtgående konsekvenser för den finansiella stabiliteten. Detta genom att attacken sannolikt påverka flera delar av det finansiella systemet samtidigt. • Vissa tredjepartstjänster (t ex Bank-id och Swish) är också lockande mål eftersom driftsavbrott skulle kunna ha omedelbar påverkan på ett stort antal personer.
Försäkringsföretag	Medium	Medium till Hög	• Ett angrepp på ett försäkringsföretag skulle sannolikt inte utgöra ett omedelbart hot mot den finansiella stabiliteten. • Försäkringsföretag har tillgång till känslig information om privatpersoner och företag vilket kan göra dem till ett lockande mål för en cyberattack.
Filialer till internationella banker	Medium	Medium	• En filial till en utländsk bank i Sverige kan visserligen fungera som en kanal för att sprida ett angrepp till andra länder. Filialerna är dock mindre attraktiva som potentiella mål och ett angrepp på dem är ett mindre hot mot den finansiella stabiliteten.

Bildkälla: Oliver Wyman, Combatting the Cyber Threat in Sweden - An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector.

Bristen på historisk erfarenhet gör det alltså svårt att slå fast vilken grad av systemriskpotential som cyberattacker kan ha. Men även *om* det skulle vara mindre sannolikt att en enstaka cyberhändelse kan få det finansiella systemet att kollapsa, är det rimligen betydligt mer sannolikt att en serie eller kombination av incidenter – sammanlänkade eller oberoende av varandra – innebär risk för stora problem i hela systemet eller i någon av dess centrala funktioner. I ett sådant scenario kan det med andra ord handla om att funktionsförmågan och förtroendet succesivt eroderar, snarare än att systemet plötsligt kollapsar på det sätt man oftast förknippar med finanskriser. Som påpekats kan även icke-systemhotande störningar skapa stora samhällsekonomiska kostnader. Om företagen själva inte har förmåga eller incitament att hantera sådana problem har reglering och tillsyn definitivt en uppgift att fylla.

Även vid en försiktig bedömning finns det alltså fog för en slutsats att systemriskaspekter sannolikt finns, och att det är än mer sannolikt att det finns risker för negativa externaliteter av mindre spektakulärt slag, men som ändå är samhällsekonomiskt betydelsefulla. Därmed finns samma grundläggande motiv för FI att agera på detta område som när det gäller risken för en traditionell finanskris.

3. Verktyg

Allmänt om verktyg för att stärka den finansiella stabiliteten
Statens roll när det gäller finansiell stabilitet handlar dels om att så långt som möjligt förebygga problem som kan bli systemhotande, dels att ha beredskap för att kunna hantera en krissituation om den ändå inträffar. För en tillsynsmyndighet som FI ligger tyngdpunkten i verksamheten på det förebyggande arbetet – tillsynsåtgärder inom ramen för de finansiella regelverken är sällan lämpliga redskap för att hantera akuta krissituationer. Dessa åtgärder syftar snarare till att se till så att olämpliga företag inte får tillstånd att driva finansiell verksamhet samt att de företag som får tillstånd har tillräcklig motståndskraft mot de risker som deras verksamhet är förknippad med.

Det finns ett antal typer av verktyg som staten kan använda för att förebygga risker som kan bli ett hot mot systemets stabilitet, mot centrala konsumentintressen eller mot finansmarknadernas generella funktionsförmåga. Oftast handlar det om att på olika sätt korrigera de avvikelser som kan uppstå mellan vad som är rationellt från ett enskilt företags eller en enskild branschs horisont, och vad som är rationellt för samhällsekonomin, det vill säga vad som i ekonomisk-teoretiska sammanhang kallas att internalisera externa effekter. Ett sätt att korrigera dessa avvikelser är att påverka företagens incitament att begränsa och bättre hantera risker. Det kan handla om direkta finansiella faktorer som exempelvis skatter och kapitalkrav, men också om mer subtila former av påverkan, på engelska kallat *moral suasion*. Det kan då handla om mer eller mindre uttryckliga hot om regleringar och ingripanden, eller om opinionsbildning.

Ett alternativt – eller kompletterande – sätt är att via reglering öka motståndskraften i företagen och i systemet genom att ställa krav på kapital, likviditet, diversifierad utlåning och liknande. En tredje väg är att via reglering och tillsyn ställa krav på de finansiella företagens organisatoriska förhållanden och transparens, kopplande till hur riskhanteringen – finansiell och operativ – är dimensionerad och organiserad. Krav ställs då också på företagens hantering av intressekonflikter samt deras information till myndigheter, allmänhet och kunder. Ytterligare ett verktyg kan vara att underlätta för företagen att kunna samarbeta och utbyta information i branschgemensamma frågor, det vill säga att främja en mer eller mindre långtgående självreglering som bidrar till att uppfylla samhällets mål med en mindre grad av statliga interventioner.

Kan verktygen användas för cyberrisker?
Alla dessa typer av verktyg kan givetvis vara relevanta även när det gäller att hantera cyberrisker. I samtliga fall finns det dock också viktiga frågetecken när det gäller användbarheten. För att rätta till incitamenten behövs någon form av uppskattning av karaktär och storlek på de negativa externa effekter som varje aktör eller funktion skapar. I synnerhet är det mycket svårt att göra en kvantitativ bedömning av dessa effekter.

Finansiella krockkuddar är visserligen till hjälp i alla typer av krissituationer, men det är inte uppenbart att till exempel en stor kapitalbuffert är avgörande för ett finansiellt företags förmåga att överleva en cyberattack. Både krockkuddar i form av kapitaltäckning och finansiella krisåtgärder i form av exempelvis statliga garantier fyller flera funktioner. Dels har dessa åtgärder genom sin blotta existens en signalfunktion och en förtroendeskapande funktion[11], dels innebär de faktiska resurser som kan användas för att köpa tid och i bästa fall överbrygga tillfälliga problem. När det gäller cybersäkerheten i finansiella företag bör det vara möjligt att – kanske som ett komplement till finansiella buffertar - exempelvis ställa krav på en viss nivå av redundans i de företagens it-system.

Reglering och tillsyn av intern styrning, kontroll och beteenden kräver idealt att tillsynsmyndigheten har en god överblick över möjliga så kallade attackvektorer, det vill säga företagens sårbarheter för olika slags attacker och hur företagens tekniska sammanlänkningar ser ut. Klart är att kunskaperna om detta kan och bör förbättras. Men det är inte realistiskt att FI, eller någon annan myndighet, skulle kunna uppnå och upprätthålla en tillräcklig kunskapsnivå på hela detta område, i synnerhet som det handlar om väldigt rörliga mål. Det är mot den bakgrunden av avgörande betydelse att företagen i den finansiella sektorn har en god förmåga att själva systematiskt arbeta med sin motståndskraft mot cyberhot.

En cyberattack utspelar sig sannolikt oftast inom en komprimerad tidsrymd, vilket innebär ett behov av informationsdelning i realtid. Problemet är att även de privata aktörerna i ett krisläge lär ha brist på information om hur och varifrån en cyberattack har initierats och spridits. I en krissituation är därför inte informationsdelning och andra former av samarbeten nödvändigtvis en tillräcklig lösning på ett genuint problem med informationsbrist. Även här kan man fundera över möjligheten att etablera redundans i strategiska delar av systemet som skulle kunna begränsa de omedelbara skadorna och köpa tid.

Allt detta pekar mot att delvis nya typer av krav kan behöva ställas på de finansiella företagen. Detta kan i sin tur kräva att regler ändras och att nya verktyg utvecklas för FI - och sannolikt även för andra myndigheter - både för att kunna arbeta förebyggande och krishanterande på ett effektivt sätt. Det kan dock vara relevant att i detta sammanhang redogöra för de verktyg som i dagsläget står FI till buds för att hantera cyberrisker i den svenska finansiella sektorn.

FI:s nuvarande verktyg

Krishantering

När det gäller krishanteringen har FI en roll som informationsnav. Genom den löpande marknadsövervakningen och företagens skyldighet att omedelbart

[11] Till exempel det så kallade kapitaltillskottsprogrammet under krisen 2008-09. Rent finansiellt utnyttjades inte detta i någon större utsträckning, men det är ganska uppenbart att det bidrog till att öka förtroendet och därigenom värna stabiliteteten.

rapportera allvarligare problem till FI, kan vi få en uppfattning om vilken karaktär störningarna har och hur allvarliga de är, och inte minst om det handlar om företagsspecifika problem eller om systemproblem. FI:s roll i ett krishanteringsskede är därför främst att analysera och vidarebefordra relevant information till andra aktörer.

Tillsyn enligt befintlig sektorslagstiftning

Ett grundläggande verktyg för att åstadkomma en hög cybersäkerhet hos företagen i den finansiella sektorn är tillsyn. Med tillsyn menas här att en aktör (en myndighet eller någon annan) får ett mandat att se till så att en annan aktör uppfyller vissa särskilt angivna krav på sin verksamhet. Inom den finansiella sektorn är tillsynen ofta nära kopplad till det verksamhetstillstånd som företaget behöver för att driva sin verksamhet. FI har som nämnts sedan länge arbetat med cyberrisker i den löpande tillsynen av de enskilda finansiella företagen och inom ramen för tillsynen av operativa risker.[12]

Genom att pröva om ett visst företag ska beviljas tillstånd att driva finansiell verksamhet tar FI ställning till om företaget och dess ledning är lämpade att driva den aktuella verksamheten. På så vis kan vi förhindra olämpliga företag från att driva finansiell verksamhet. FI kan dessutom ingripa mot företag som bryter mot de regler som gäller för verksamheten, ytterst genom att återkalla tillståndet. Inom ramen för den löpande tillsynen har FI tämligen vidsträckta befogenheter. FI kan exempelvis begära att ett företag eller någon annan tillhandahåller uppgifter, handlingar eller något annat eller att den som förväntas kunna lämna upplysningar i saken kommer till förhör. FI kan även göra platsundersökningar.

När det gäller tillsynen över cybersäkerheten inom den svenska finansiella sektorn utgår FI från en hel palett med olika former av regler. Gemensamt för dessa regler är att de kan ge FI en möjlighet att ingripa med sanktioner mot företag som inte följer reglerna, ytterst genom att återkalla verksamhetstillståndet. Tillsynen ger oss även en möjlighet att löpande undersöka om företagen följer tillämpliga regler. Ett generellt krav som gäller för finansiella företag är att de ska identifiera och ha kontroll över de risker som är förknippade med den rörelse som företaget driver. Inom ramen för detta krav ryms givetvis att de finansiella företagen ska identifiera och kontrollera risken för att de, eller någon av deras leverantörer, utsätts för en cyberattack. Här nedan ger vi en översikt över dessa regler.[13]

När det gäller FI:s tillsyn över kreditinstitut (banker- och kreditmarknadsföretag) finns den grundläggande bestämmelsen i 6 kap. 2 §

[12] FI-rapporterna från område Bank respektive Försäkring 2018–19.
[13] Det bör även nämnas att Financial Stability Board och andra internationella organ löpande tar fram olika rekommendationer och rapporter om cybersäkerheten i finansiella företag.

lagen om bank- och finansieringsrörelse.[14] Bestämmelsen innehåller en generell skyldighet för kreditinstitut att identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som dess rörelse är förknippad med. Relevanta regler finns även i FI:s föreskrifter och allmänna råd.[15] Därutöver har den Europeiska bankmyndigheten (EBA) utfärdat riktlinjer för hantering av risker kopplade till företags informations- och kommunikationsrisker (IKT-risker) och säkerhetsrisker samt för utkontraktering.[16]

När det gäller försäkringsföretag finns det grundläggande bestämmelser i försäkringsrörelselagen om hur cyberrisker ska hanteras. Lagens tionde kapitel innehåller bestämmelser om företagsstyrning, varav flera är relevanta när det gäller företagens cybersäkerhet. Här finns bland annat bestämmelser om riskhantering, kontinuitetshantering och uppdragsavtal. Dessa bestämmelser kompletteras av bestämmelser i kommissionens delegerade förordning om komplettering av Solvens II samt riktlinjer utfärdade av den Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa).[17]

För aktörerna på värdepappersmarknaden finns det flera olika regelverk som berör cybersäkerhet. Utgångspunkten för mycket av regleringen för aktörer inom den finansiella infrastrukturen är principerna för finansmarknadsinfrastrukturer, *Principles for Financial Market Infrastructures* (PFMI), som har tagits fram gemensamt av den Internationella organisationen för värdepapperstillsyn (Iosco) och Banken för internationell betalningsutjämning (BIS).

När det gäller centrala motparter och värdepapperscentraler finns relevanta regler för företagsstyrning i EU:s förordning om OTC-derivat, centrala motparter och transaktionsregister (Emir-förordningen) respektive EU:s förordning om förbättrad värdepappersavveckling och om värdepapperscentraler (CSDR-förordningen).[18] I kraven på adekvat företagsstyrning ingår att företagen ska ha förmågan att kunna identifiera och hantera risker, däribland cyberrisker, i sin verksamhet. Därutöver innehåller lagen om värdepappersmarknaden (LV) liknande bestämmelser för

---

[14] En mer fullständig beskrivning av FI:s verktyg när det gäller bankernas arbete med cybersäkerhet finns i FI:s tillsynsrapport nr 9, Bankernas arbete med informations- och cybersäkerhet, 2018.
[15] Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut, Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker och Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.
[16] EBA/GL/2019/04 samt EBA/GL/2019/02 riktlinjer för utkontraktering. Riktlinjer från EBA, eller en av de andra europeiska tillsynsmyndigheterna, är inte formellt bindande men de berörda företagen ska söka följa dem med alla tillgängliga medel. IKT är en förkortning för informations- och kommunikationsteknik.
[17] Se artiklarna 258–260 samt 274 i Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (Solvens II) samt Eiopas riktlinjer för företagsstyrningssystem (EIOPA-BoS-14/253).
[18] Artikel 26 respektive artikel 45.

värdepappersbolag (8 kap. 4 §), börser (13 kap. 2 §) och clearingorganisationer (20 kap. 1 §). Även här fylls lagreglerna ut av FI:s föreskrifter.[19] Det kan vara värt att notera att regler om cybersäkerhet saknas för vissa handelsplatser för finansiella instrument (MTF-plattformar), fondförvaltare och alternativa fondförvaltare.

Sammanfattningsvis kan vi konstatera att regelverken kring cyberrisker skiljer sig åt mellan olika sektorer av den svenska finansiella sektorn.

Ett exempel: FI:s underökningar av Nasdaqbolagen
Sommaren 2015 inledde FI undersökningar av Nasdaq Stockholm AB och Nasdaq Clearing AB (Nasdaqbolagen). Undersökningarna fokuserade på hur företagen hanterar cyberrisker. Eftersom bland annat funktionen för informationssäkerhet var utkontrakterad till koncernens moderbolag Nasdaq, Inc., undersökte FI hur företagens självständighet och oberoende såg ut.

I december 2016 meddelade FI:s styrelse sina beslut: att ge Nasdaq Stockholm AB en anmärkning och en sanktionsavgift på 30 miljoner kronor, och att ge Nasdaq Clearing AB en anmärkning och en sanktionsavgift på 25 miljoner kronor. Sanktionerna motiverades av att Nasdaqbolagen inte haft tillräcklig självständig kompetens och inte heller försett sig med den information som behövs för att kunna bedöma de levererade tjänsternas kvalitet och därmed kunna ställa tillräckliga krav på leverantören.

Nasdaqbolagen överklagade FI:s beslut. Det slutliga avgörandet i ärendet kom i augusti 2020.[20] Förvaltningsrätten upphävde då FI:s beslut eftersom den ansåg att det hade saknats laglig grund för FI att ingripa mot bolagen. Anledningen är att domstolen ansåg att den allmänna regeln i 13 kap. 1 § LV inte kunde ges en så pass vidsträckt tolkning att den omfattar de grunder som FI byggde sanktionsbesluten på.

Tillsyn över samhällsviktiga tjänster enligt NIS-direktivet
År 2016 antog EU det så kallade NIS-direktivet.[21] Syftet med direktivet är att höja nivån för cybersäkerheten i flera olika sektorer. I Sverige har direktivets bestämmelser genomförts främst genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster som trädde i kraft 2018. Lagen omfattar leverantörer som tillhandahåller en samhällsviktig tjänst i Sverige. Vilka dessa leverantörer är har det uppdragits åt Myndigheten för samhällsskydd och beredskap (MSB) att avgöra. Av MSB:s föreskrifter

[19] Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker, Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem samt Finansinspektionens allmänna råd (FFFS 2005:1) allmänna råd om styrning och kontroll av finansiella företag.
[20] Förvaltningsrätten i Stockholms dom den 25 augusti 2020 i mål 25434-19. FI har valt att inte överklaga avgörandet som därmed vunnit laga kraft.
[21] Europaparlamentets och Rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

(MSBFS 2018:7) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster framgår vilka leverantörer som är samhällsviktiga.

Det är särskilt två kategorier som är av intresse i detta sammanhang: bankverksamhet och finansmarknadsinfrastruktur. När det gäller bankverksamhet omfattas de kreditinstitut som enligt FI:s årliga tillsynskategorisering tillhör kategori 1 eller 2, eller utländska kreditinstitut som driver finansieringsrörelse i Sverige genom en filial med en balansomslutning på minst 500 miljarder kronor.[22] Vad gäller finansmarknadsinfrastruktur omfattas den som tillhandahåller en handelsplats med en sammanlagd handelsomsättning på minst 1 miljard kronor per dag, eller tjänster som utförs av centrala motparter. De företag som omfattas av denna lagstiftning är skyldiga att bland annat utföra ett systematiskt och riskbaserat informationssäkerhetsarbete samt att rapportera incidenter. Vid en överträdelse av dessa skyldigheter har den ansvariga tillsynsmyndigheten möjlighet att utfärda åtgärdsföreläggande eller sanktionsavgift.

I december 2020 föreslog Europeiska kommissionen ett nytt NIS-direktiv, som innebär än mer långtgående skyldigheter för medlemsstaterna när det gäller skyddet för leverantörer av samhällsviktiga tjänster.[23] Bland annat innebär det nya NIS-direktivet förstärkta regler om incidentrapportering samt att fler företag inom den finansiella sektorn kan komma att omfattas av dess regler. Samtidigt med förslaget om det nya NIS-direktivet föreslog Kommissionen ett nytt direktiv om kritiska enheters motståndskraft (CER-direktivet) som även det kommer att omfatta vissa finansiella företag. [24] De två föreslagna direktiven medför liknande krav på rapportering och riskanalyser för de företag som omfattas.

Uppdaterad säkerhetsskyddslag

Sedan den 1 april 2019 gäller en säkerhetsskyddslagstiftning i Sverige som innebär skyldigheter för den som driver säkerhetskänslig verksamhet.[25] I korthet innebär lagen att både offentliga och privata verksamhetsutövare är skyldiga att utreda behovet av säkerhetsskydd i sin verksamhet samt att planera och vidta de åtgärder som behövs. Verksamhetsutövaren ska bland annat förebygga skadlig inverkan på uppgifter och informationssystem samt att säkerhetsskyddade uppgifter röjs.

---

[22] Se FI:s årliga tillsynskategorisering av svenska kreditinstitut och utländska kreditinstituts svenska filialer. Vad gäller de banker som driver filialverksamhet i Sverige använder sig FI av kategoriseringen filial, betydande filial samt särskilt betydande filial. Se Tillsynskategorisering av svenska kreditinstitut och utländska kreditinstituts svenska filialer för 2021 (FI dnr 20-1930).

[23] Se Förslag till Europaparlamentets och Rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM/2020/823 final.

[24] Se Förslag till Europaparlamentets och Rådets direktiv om kritiska entiteters motståndskraft, COM(2020) 829 final.

[25] Säkerhetsskyddslag (2018:585) samt säkerhetsskyddsförordning (2018:658).

År 2018 presenterades en statlig utredning ett förslag till uppdaterad säkerhetsskyddslag.[26] Enligt detta uppdaterade förslag får FI i uppdrag att utöva tillsyn över säkerhetsskyddet hos finansiella företag och motsvarande utländska företag som är etablerade i Sverige.[27] Utredningens förslag har remitterats och bereds för närvarande. En proposition väntas under våren 2021.

Dora-förordningen
Den 24 september 2020 presenterade Europeiska kommissionen ett förslag i form av en förordning för att stärka finansmarknadens operationella motståndskraft beträffande cyberrisker (Dora-förordningen).[28] Huvudmotivet är dels ett ökat behov av reglering och tillsyn i ljuset av den växande sårbarheten för cyberrisker, dels ett behov av större enhetlighet i regelverken, både mellan delsektorer och mellan jurisdiktioner. Den föreslagna regleringen riktar sig till i princip alla de typer av företag som i dag står under FI:s tillsyn. Den föreslagna förordningen innehåller ett generellt krav för dessa företag att ha kontroll över samtliga it-relaterade risker.

Förordningen ställer långtgående krav på de finansiella företagen att ha tillräckliga system och styrdokument på plats för att hantera dessa risker. Dessutom innehåller förslaget regler som tydliggör de finansiella företagens ansvar även för den del av it-verksamheten som har delegerats till tredje part. De europeiska tillsynsmyndigheterna får i uppdrag att övervaka de tredjeparts-leverantörer som bedöms som ”kritiska”. Genom denna förordning skapas mer enhetliga regler för aktörerna inom den europeiska finansiella sektorn. Förordningen kommer nu att bli föremål för förhandlingar mellan Europaparlamentet och medlemsstaterna.

Kategorisering av verktyg
Utifrån översikten ovan går det att dela verktygen i följande tre kategorier:

1. **Ordinära tillsynsverktyg.** Inom denna kategori ryms de verktyg som är en del av den ordinära tillsynen över finansiella företag, främst utifrån krav i relevant sektorslagstiftning när det gäller intern styrning och kontroll. Här ryms även regler om ägar- och ledningsprövning samt kapitalkrav. Syftet med dessa verktyg är att se till så att de finansiella företagen har kunskap om och förmåga att hantera alla de risker som dess verksamhet medför. Även om verktygen används för att se till så att motståndskraften mot cyberattacker är hög, är de i stort desamma som vid övrig tillsyn.

[26] SOU 2018:82 Kompletteringar till den nya säkerhetsskyddslagen.
[27] Dessa företag omfattas redan i dag av lagens bestämmelser men står under länsstyrelsernas tillsyn. Utredningen kunde dock konstatera att länsstyrelserna ”i princip inte genomfört någon tillsyn” (s. 371).
[28] Förslag till Europaparlamentets och Rådets Förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, COM(2020) 595 final.

2. **Särskilda krav på finansiella företag när det gäller cyberrisker**. Inom denna kategori ryms de särskilda krav som bör uppställas mot finansiella företag för att hantera cyberrisker, exempelvis krav på incidentrapportering. Bland dessa verktyg bör tillsyn gällande ledningssystem för informationssäkerhet, uppdragsavtal, kontinuitetshantering, redundans i system samt genomförande av tester nämnas.

3. **Tillsyn över tredjepartsleverantörer**. En särskild typ av verktyg när det gäller arbetet mot cyberrisker avser tillsynen över de så kallade tredjepartleverantörerna. Denna typ av företag har på senare tid tagit över allt fler av de uppgifter som de finansiella företagen själva tidigare utfört. På så vis har möjligheterna till tillsyn över dessa företag blivit allt mer aktuell.

   En tredjepartsleverantör är ett – ofta icke-finansiellt – företag som utför olika it-relaterade tjänster åt ett finansiellt företag.[29] Dessa företag är inte sällan stora globala företag som utför tjänster åt ett stort antal finansiella och icke-finansiella företag.[30] Även om dessa företag inte driver tillståndspliktig finansiell verksamhet är det viktigt att se till att de har en tillräcklig motståndskraft mot cyberattacker eftersom en omfattande attack mot en sådan leverantör kan få mycket stora konsekvenser för flera finansiella företag och därmed även för det finansiella systemet.

   Det faktum att dessa tredjepartsleverantörer ofta är större företag med global verksamhet kan innebära vissa svårigheter för en enskild nationell tillsynsmyndighet att utöva tillsyn över dem. En effektiv tillsyn kräver sannolikt ett nära samarbete mellan tillsynsmyndigheter i flera olika länder. En annan utmaning är att dessa leverantörer kan ligga utanför EU, vilket för med sig en särskild tredjelandsproblematik till exempel vid likvärdighetsbedömningar eller tillämpningen av unionsrättsliga regelverk om personuppgifter.

4. Samverkan mot cyberattacker

Att motverka cyberattacker är ett ansvar som generellt ligger på den som utövar en viss verksamhet.[31] Syftet med detta kapitel är att ge en bild av

[29] I EBA:s riktlinjer för utkontraktering (EBA/GL/2019/02) benämns tredjepartsleverantörer som tjänsteleverantör vilket definieras som ”en tredje part som tar på sig en utkontrakterad process, tjänst eller verksamhet, eller delar därav, enligt ett arrangemang för utkontraktering.
[30] Dock ska noteras att det också finns mindre, nischade företag vars tjänster kan vara av stor betydelse för branschen
[31] När det gäller myndigheter föreskrivs det i 19 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap att varje myndighet har ett ansvar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. När det gäller finansiella företag finns det krav i såväl lagstiftning som i föreskrifter från de

ansvarsfördelningen mellan myndigheter i Sverige när det gäller arbetet mot cyberattacker riktade mot den finansiella sektorn. I kapitlet behandlas även de strukturer för offentlig-privat samverkan som finns på plats. Avslutningsvis innehåller kapitlet en kortare internationell utblick.

Samhällets arbete för cybersäkerhet

År 2018 antog riksdagen en nationell strategi för samhällets informations- och cybersäkerhet.[32] Syftet med strategin är att den ska vara en plattform för Sveriges fortsatta utvecklingsarbete inom området. Strategin ska bidra med förutsättningar till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. I det följande beskriver vi kort det svenska samhällets arbete för cybersäkerhet med fokus på den finansiella sektorn.

MSB och Säkerhetspolisen

I Sverige finns det flera myndigheter som har ett allmänt ansvar för cybersäkerheten i samhället. MSB har regeringens uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet samt att analysera och bedöma omvärldsutvecklingen inom området. I detta uppdrag ingår att lämna råd och stöd om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.[33] MSB ska även ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Inom ramen för detta uppdrag ska myndigheten bl.a. samverka med de myndigheter som har särskilda uppgifter inom informations-säkerhetsområdet.[34] MSB ger även ut föreskrifter om it- och informationssäkerhet.

När det gäller frågor om säkerhetsskydd har Säkerhetspolisen ett viktigt uppdrag. Myndigheten har i uppdrag att utöva tillsyn över bland annat FI:s skyldigheter enligt säkerhetsskyddslagstiftningen. Därutöver bereds för närvarande ett förslag till en uppdaterad säkerhetsskyddslagstiftning som skulle innebära att Säkerhetspolisen, tillsammans med Försvarsmakten, får ett samordnande ansvar. Detta skulle innebära att myndigheterna bland annat får i uppdrag att utveckla metodstöd för tillsynen samt verka för erfarenhetsutbyten mellan de olika tillsynsmyndigheterna.[35]

Bland de myndigheter som har ett särskilt ansvar inom informationssäkerhetsområdet märks även Försvarsmakten, Försvarets

---

europeiska tillsynsmyndigheterna och från FI om hur de ska hantera risker för cyberattacker i sin respektive verksamhet. De finansiella företagens ansvar för att hantera risker kopplade till cyberattacker och FI:s möjligheter att utöva tillsyn över denna riskhantering kommer att behandlas i ett senare kapitel.

[32] Nationell strategi för samhällets informations- och cybersäkerhet, Skr. 2016/17:213.

[33] 11 a § förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

[34] 11 b § förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

[35] Se SOU 2018:82 Kompletteringar till den nya säkerhetsskyddslagen. s. 356 ff.

materielverk (FMV), Försvarets radioanstalt (FRA), Post- och telestyrelsen (PTS), Polismyndigheten och Säkerhetspolisen. Dessa myndigheter ingår i Samverkansgruppen för informationssäkerhet (SAMFI) som leds av MSB. Den huvudsakliga uppgiften för gruppen är att tillsammans genomföra de förslag på åtgärder som årligen tas fram inom ramen för den nationella handlingsplanen för samhällets informationssäkerhet.

Samarbete kring tillsynen enligt NIS-direktivet
Som nämnts ovan har FI ansvar för viss tillsyn enligt bestämmelserna i NIS-direktivet. MSB ansvarar för att koordinera arbetet mellan de myndigheter som ansvarar för att utöva tillsyn enligt NIS-direktivet. [36] Av NIS-direktivet följer även att varje medlemsstat ska etablera en så kallad *Computer Security Incident Response Team* (CSIRT) som är en särskild funktion som ska underlätta informationsutbytet och samverkan mellan medlemsstaterna. Som nationell kontaktpunkt för NIS-direktivet och den nationella CSIRT-enheten, deltar MSB i olika internationella forum, såsom NIS-Cooperation Group och CSIRT's Network, för att bevaka och bidra till NIS-direktivets utveckling i EU.[37]

Ett nytt center för cybersäkerhet
År 2019 beslutade regeringen att ett myndighetsgemensamt nationellt cybersäkerhetscenter ska byggas upp. Centret ska bestå av Försvarets Radioanstalt (FRA), MSB, Försvarsmakten och Säkerhetspolisen och kommer att stödja det förebyggande arbetet för de mest skyddsvärda verksamheterna i samhället.[38] Samverkan med privata och offentliga aktörer kommer också att vara en central del i centrets uppgifter och verksamhet. Centret började byggas upp 2020 och ska vara fullt fungerande 2025.[39]

FI:s roll inom totalförsvaret
År 2015 beslutade regeringen att återuppta en sammanhängande planering för totalförsvaret. Ett led i detta arbete är att ge flera myndigheter ett särskilt ansvar inom totalförsvaret. Regeringen har utsett FI till bevakningsansvarig myndighet. Det innebär att FI är skyldig att analysera om det finns sårbarheter eller hot och risker inom myndighetens ansvarsområde.

De bevakningsansvariga myndigheterna ska även planera för att kunna anpassa verksamheten inför en förändrad säkerhetspolitisk situation. Förordningen innehåller mer preciserade skyldigheter för dessa myndigheter. Bland dessa skyldigheter märks bland annat att myndigheterna ska samverka med övriga berörda statliga myndigheter, kommuner, regioner, sammanslutningar och

[36] 17 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster.
[37] Se Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022: redovisning 2020. Sveriges nationella CSIRT är Cert.se som har till uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter.
[38] De nämnda myndigheterna har ingått en överenskommelse om fördjupad samverkan med Polismyndigheten, PTS och FMV.
[39] Svar på uppdrag (Fö2019/01000/SUND) inför inrättandet av ett nationellt cybersäkerhetscenter den 19 december 2019. Se även 2020/21:1, utgiftsområde 6, s. 14.

näringsidkare.För att underlätta samordningen mellan myndigheterna har regeringen grupperat de bevakningsansvariga myndigheterna i samverkansområden.[40] FI ingår i samverkansområdet Ekonomisk säkerhet.[41]

Utredningen om civilt försvar

Den 1 mars 2021 presenterade Utredningen om civilt försvar sitt slutbetänkande.[42] I betänkandet föreslår utredningen att samverkansområdena avvecklas och ersätts av tio beredskapssektorer och fyra särskilda beredskapsområden. I dessa ingår myndigheter med ansvar för verksamheter och funktioner som är särskilt viktiga att upprätthålla under kris, höjd beredskap och ytterst i krig. En myndighet i varje beredskapssektor föreslås få ett mandat att inrikta och samordna arbetet inom sektorn, en sektorsansvarig myndighet.

Utredningen föreslår att FI blir sektorsansvarig myndighet för beredskapssektorn Finansiella tjänster. Utöver FI föreslås sektorn bestå av Riksgälden samt av Riksbanken som adjungerad medlem. Skulle detta förslag bli verklighet innebär det krav på FI att hålla ihop sektorns planering för höjd beredskap och för fredstida kriser som kan drabba sektorn såsom en omfattande cyberattack. Den sektorsansvariga myndigheten föreslås även ansvara för att det byggs upp en kapacitet inom sektorn för att operativt kunna hantera såväl krissituationer som höjd beredskap och att ansvara för kontakten med övriga sektorer och beredskapsområden.

Utredningen föreslår även att ett särskilt beredskapsområde för cybersäkerhet inrättas bestående av ett samarbete mellan Säkerhetspolisen, MSB, Försvarsmakten och FRA.

Samarbetsorgan inom cybersäkerhetsområdet

Det finns i dagsläget flera olika forum som samlar såväl privata som offentliga aktörer med ett ansvar inom cybersäkerhetsområdet. En del av dessa har en mer generell inriktning mot cybersäkerhet, medan andra är inriktade på finansiell stabilitet. Här nedan redogörs kort för några av de mer centrala samarbetsorganen.

På MSB finns cybersäkerhetsrådet som samlar representanter från ett antal myndigheter, lärosäten och från näringslivet. Varken FI eller någon annan myndighet med särskilt ansvar för finansiell stabilitet ingår i rådet. Cybersäkerhetsrådets arbete syftar bland annat till att rådets medlemmar ska informera varandra om utvecklingstrender samt att de ska ge synpunkter på och kvalitetssäkra MSB:s arbete på området.

[40] 7 § Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.
[41] Övriga myndigheter i samverkansområdet är Försäkringskassan, MSB, Pensionsmyndigheten, Riksgäldskontoret och Skatteverket. Riksbanken deltar i arbetet som adjungerad.
[42] SOU 2021 Struktur för ökad motståndskraft.

MSB administrerar även fem olika sektorsspecifika forum för informationsdelning om informationssäkerhet, benämnda FIDI. Syftet med dessa forum är att utbyta information om hot, sårbarheter och incidenter mellan relevanta myndigheter och privata aktörer. Ett av dessa forum, FIDI-Finans, fokuserar på den finansiella sektorn. Där ingår representanter för de större svenska bankerna, finansiella infrastrukturföretag, Riksbanken, Riksgälden, Polisen och FRA.[43] FI har beslutat sedan tidigare att inte ingå i detta forum. Vi deltar dock i Samverkansområdet ekonomisk säkerhet (SOES) som är ett samverkansforum med fokus på att se till så att de system som finns i samhället för att genomföra betalningar är robusta. SOES leds av MSB och består av sammanlagt åtta myndigheter.[44]

Ytterligare ett viktigt samverkansorgan är Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS). FSPOS bildades 2005 och är ett frivilligt samverkansforum med deltagare från myndigheter – däribland FI – samt näringslivet inom finanssektorn. FSPOS har en fast organisation med tre nivåer, fullmäktige, styrelse och arbetsgrupper, där FI är representerat i samtliga. FSPOS:s verksamhet finansieras genom att de organisationer som ingår står för kostnaderna för egna medarbetare som deltar i arbetet. Syftet med verksamheten är att privata och offentliga organisationer inom finanssektorn ska arbeta för att förbättra förmågan att förebygga, förbereda och snabbt återhämta sig från operativa kriser. FSPOS:s arbete fokuserar alltså inte bara på cybersäkerhet, även om frågan är central för organets verksamhet.[45]

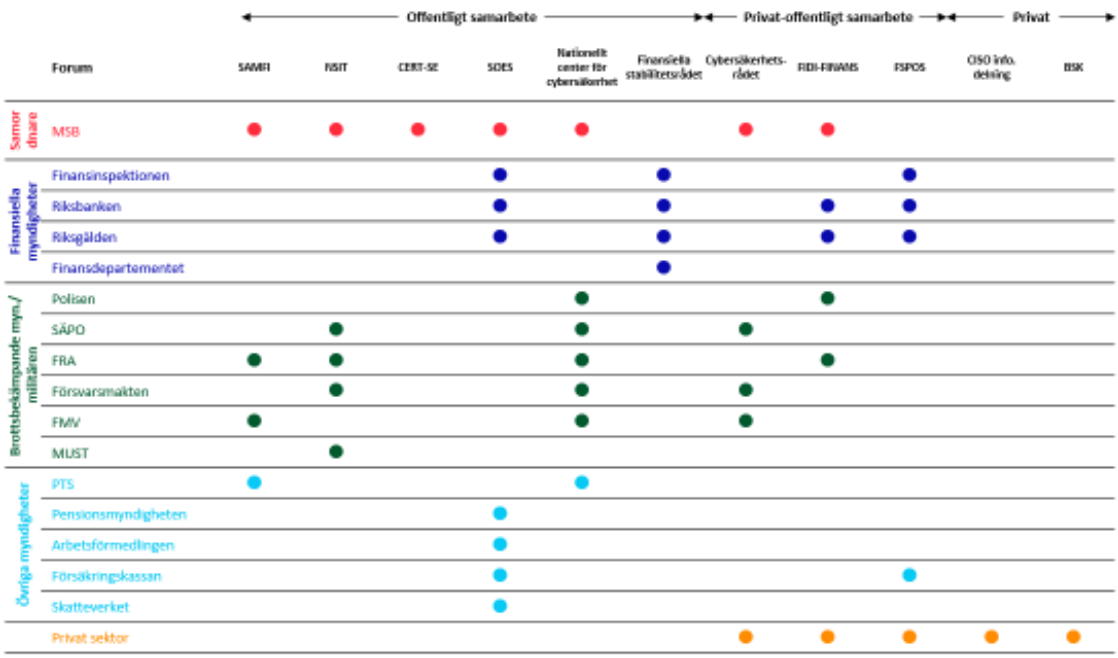
Fyra svenska myndigheter har ett särskilt ansvar för att verka för ett stabilt finansiellt system. Dessa myndigheter är Riksgälden, Riksbanken, Regeringskansliet (Finansdepartementet) samt FI. Även om myndigheterna har ett gemensamt ansvar har de olika uppgifter och verktyg för att utföra sina uppgifter. Myndigheterna ingår i Finansiella stabilitetsrådet, ett diskussionsforum för frågor som rör finansiell stabilitet och hur man kan motverka finansiella obalanser. Eftersom frågor om cyberattacker mot finansiella företag kan påverka den finansiella stabiliteten i Sverige, har rådet diskuterat frågor om cybersäkerheten i den finansiella sektorn.

[43] Mer information om de samverkansorgan som MSB administrerar finns på myndighetens webbplats, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samverkan-inom-informationssakerhet/ (läst 2021-02-21).
[44] Mer information om SOES finns på MSB:s webbplats, https://www.msb.se/sv/publikationer/samverkansomradet-ekonomisk-sakerhet-soes/ (2021-02-21).
[45] Se FSPOS:s verksamhetsplan för 2021 samt dess strategiska plan för 2020–2023.

Bilden nedan illustrerar de samverkansgrupper som finns i dag och som arbetar med frågor om cybersäkerhet inom den svenska finansiella sektorn.[46]

	Forum	Samordnare	Beskrivning
Offentliga samarbetsforum	SAMFI (Samverkan inom informationssäkerhet)	MSB	Fyra myndigheter som har särskilda uppgifter inom ramen för den nationella cybersäkerhetsstrategin – ansvarig för strategiverkställandet
	NSIT (Nationell samverkan till skydd mot allvarliga IT-hot)	MSB	Samarbete mellan brottsbekämpande myndigheter och militären – analyserar och utvärderar hot och svagheter
	CERT-SE (Swedish Computer Security Incident Response Team)	MSB	Stödjer myndigheter, företag och kommuner med cyberincidenter och publicerar varningar och råd om svagheter
	SOES (Samverkansområdet Ekonomisk Säkerhet)	MSB	Ej direkt fokus på cyberrisk men arbetar för tillgång till och förtroende för betalningar, särskilt från samhällsperspektiv
	Nationellt center för cybersäkerhet	MSB	Fullt verksam 2025, kommer att ta fram analyser, sprida hotinformation, samt samordna under IT incident och angrepp
	Finansiella stabilitetsrådet	Finansdepartementet	Två möten om året mellan fyra myndigheter ansvariga för den finansiella stabiliteten
Privat-Offentliga	Cybersäkerhetsrådet	MSB	Etablerades för att informera, yttra sig om och kvalitetssäkra MSB:s cybersäkerhetsarbete – inkluderar representanter från den akademiska sfären och den privata sektorn
	FIDI-FINANS (Forum för informationsdelning om informationssäkerhet i finanssektorn)	MSB	Ett av de FIDI-forum som etablerades av MSB för informationsdelning i sektorerna med högst exponering till cyberrisk (fokus på den finansiella sektorn)
	FSPOS (Finansiella Sektorns Privat-Offentliga Samverkan)	Riksbanken (roterande)	Huvudforum för privat-offentligt samarbete i den finansiella sektorn – har arbetsgrupp med fokus på cyberrisk
Privata	BSK (Bankernas Säkerhetskommitté)	Svenska bankföreningen	Kommitté med fokus på gemensamt säkerhetsarbete mellan banker Svenska Bankföreningen (inklusive cybersäkerhet)
	CISO informationsdelning	N/A	Samarbete med informell struktur med focus på cybersäkerhetsfrågor mellan informationscheferna på de stora bankerna

Bilden nedan visar i vilken utsträckning svenska myndigheter deltar i de olika samverkansforum som finns på cybersäkerhetsområdet.[47]



[46] Bildkälla: Oliver Wyman, Combatting the Cyber Threat in Sweden - An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector.
[47] Bildkälla: Oliver Wyman, Combatting the Cyber Threat in Sweden - An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector.

Sammanfattningsvis kan man konstatera att det finns ett betydande antal samarbetsorgan och forum för att analysera och motverka cyberrisker ur olika infallsvinklar. FI medverkar i dag i vissa av dessa. Det finns dock inget organ eller forum som på ett tydligt sätt anger riktningen när det gäller den finansiella sektorns arbete för att motverka cyberrisker. Framöver finns det sannolikt ett behov av en ökad samverkan mellan myndigheter och med branschföreträdare för att motverka cyberhoten mot den svenska finansiella sektorn.

Internationell utblick

Det kan i sammanhanget vara relevant att göra en utblick mot andra länder som redan har ett utvecklat samarbete mot cyberhot mot den finansiella sektorn. I **Danmark** har en nationell strategi för arbetet för cybersäkerhet antagits. Till skillnad från Sverige har det även tagits fram sektorsspecifika nationella strategier. Inom ramen för den sektorspecifika strategin för den finanssektorn, har den finansiella tillsynsmyndigheten Finanstilsynet fått i uppdrag att vara *decentral enhed for cyber- og informationssikkerhed for finanssektoren (DCIS).* Det innebär att Finanstilsynet ansvarar för de uppgifter som anges i den nämnda strategin. DCIS arbetar således med den finansiella sektorns beredskap mot cyberhet, analys av hot och sårbarheter samt kunskapsspridning.

I **Storbritannien** har branschorganisationen UK Finance, på initiativ av den brittiska centralbanken Bank of England, startat the Financial Sector Cyber Collaboration Centre (FSCCC). Syftet med att etablera detta center är att möjliggöra och förenkla samarbetet mellan offentliga myndigheter såsom Bank of England och Financial Conduct Authority (FCA) samt den privata sektorn. På så vis blir det enklare att dela information mellan företag verksamma inom den finansiella sektorn och ansvariga tillsynsmyndigheter. Genom FSCCC är det även möjligt att utbyta information med underrättelsetjänsten och brottsbekämpande myndigheter. Det är möjligt för varje deltagare inom FSCCC att bestämma i vilken utsträckning de önskar delta i samarbetet.

Singapore antog 2018 en cybersäkerhetslagstiftning som ställer strikta krav på den finansiella sektorn i landet. Landets finansiella tillsynsmyndighet, Monetary Authority of Singapore (MAS), har etablerat flera permanenta kommittéer för att samarbeta med den finansiella sektorn om cybersäkerhet. MAS har också etablerat ett rådgivande organ – Cyber Security Advisory Panel – bestående av internationella cybersäkerhetsexperter som ger råd åt såväl MAS som åt företag inom den finansiella sektorn om hur de bör arbeta med cybersäkerhet. Panelen fungerar även som ett forum för att utbyta tankar kring arbetet mot cyberhot.[48]

[48] Se https://www.mas.gov.sg/who-we-are/MAS-Advisory-Panels-and-Committees/Cyber-Security-Advisory-Panel (läst 2021-02-21).